



ANNOTATED SUBSTITUTE SPECIFICATION

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the priority of Japanese Patent Application No. 2000-347471 filed on November 15, 2000 in the Japanese Patent Office, the disclosure of which is incorporated herein in its entirety by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a network server such as a WWW server for transmitting a hypertext that is written in a language such as HTML or XML, and a transmission control method of a hypertext, and a recording medium storing a hypertext.

2. Description of the Prior Art

Figs. 10A and 10B are diagrams showing a conventional WWW system 9.

Conventionally, a WWW system is widely used as a system for accessing to an information resource that is distributed on the Internet.

The WWW system comprises a WWW server for managing the information resource to be provided for a user, a client having a WWW browsing function for accessing thereto, a HTTP placed on a layer upper than the TCP/IP as a communication protocol, and other various devices or software.

The information resource is provided as a hypertext file that is written in a language such as HTML or XML (Extensible Markup Language).

A user inputs and designates a URL of the hypertext that is desired to be accessed ~~access~~ in the WWW browser of the client. The WWW browser requests the WWW server to access ~~to~~ the hypertext, so as to download the hypertext from the WWW server to the client.

For example, if the HTTP is used as a communication protocol, the URL designating a hypertext "top.html" on a server "WWW.xxxxx.co.jp" is expressed as "http://WWW.xxxxx.co.jp/top.html."

The WWW system is used not only in the Internet but also in a LAN or an intranet connecting a plurality of LANs.

Many users use the Internet. One object of the Internet is to share information resources among many users in the world. Theoretically, any Any-client on the Internet can access to a hypertext on a WWW server ~~in principle~~.

However, recent usage of the Internet ~~becomes~~ has become increasingly diversified. There is a ~~demand-need~~ for controlling an access to a hypertext so that only specific users are permitted to access.

Some methods are proposed for controlling an access.

One of ~~them is a method of~~ is establishing a firewall using a proxy server or the like. For example, a firewall is established between an intra-company network and the Internet, so as to control the communication between them. By using the firewall, only specific users are permitted to access to the Internet from the intra-company network, or an access using a specific communication protocol is prohibited as an access control.

~~It is another~~ Another method ~~to provide~~ provides an access control file as shown in Fig. 10B in the directory where the hypertext is placed.

The WWW system 9 shown in Fig. 10A is on the Internet and comprises a WWW server 91 and clients 92 and 93.

The WWW server 91 includes a magnetic recording device 91a, in which a hypertext 91f is recorded as an information resource. The hypertext 91f in the magnetic recording device 91a is managed by a directory structure, and one directory 91d includes an access control file 91c in which information about an access control to the plural hypertexts 91f and the directories 91d thereof is described.

The clients 92 and 93 can access to the Internet by a WWW browser. As an example, ~~Here, it is supposed that~~ the client 92 belongs to a domain "xxxxx.co.jp," and the client 93 belongs to a domain "zzzzz.co.jp."

A user inputs a URL of the hypertext 91f in the WWW browser of the client 92 or 93, so as to request for an access to the hypertext 91f. This request is transmitted to the WWW server 91.

The WWW server 91 refers to the access control file 91c that is in the directory 91d where the hypertext 91f is placed and decides whether the hypertext 91f should be transmitted to the client that has made the request.

The access control file 91c shown in Fig. 10B has contents indicating ~~of~~ allowing an access from the domain "xxxxx.co.jp" and denying any access from other domains. Therefore, in this case, an access is allowed responding to a request from the client 92, and the hypertext 91f is transmitted to the client 92. On the contrary, an access is denied responding to a request from the client 93, and a message indicating the access denial is

transmitted to the client 93.

However, with the above-mentioned access control using the firewall, only an administrator can set the access control and advanced knowledge is required for the setting. If the setting is misused, the security of the entire system can be deteriorated. In addition, it is difficult to set the access control for each file. Therefore, the method using a firewall is not suitable for a ~~fine~~ precise access control.

~~The~~ A method of providing an access control file 91c can control an access for each directory, so it is often used by a service provider of the Internet who provides many users (who open a Web site and offer information resources such as Web contents) with a service. The Internet service provider gives a directory to each information provider. Each information provider stores a hypertext 91f as an information resource in his or her directory, so that many users on the Internet can share the hypertext 91f.

Since one access control file 91c is placed in one directory 91d, a uniform access control is performed for ~~the~~ all hypertexts 91f in the directory 91d. Therefore, if a different setting of the access control is desired for each hypertext 91f, a directory 91d should be provided for each hypertext 91f.

However, a directory is ~~originally a concept used~~ for making classification of file-files be easily understood for an administrator in accordance with kinds or contents of the file. The usage of the directory for the access control may complicate the file management. In addition, if the URL of the hypertext 91f is changed whenever the setting of the access control is changed in the WWW server 91, it may be ~~inconvenience~~ inconvenient for the user of the client side to access to the hypertext 91f.

Furthermore, since the access control file 91c depends on software that is used in the WWW server 91 for the access control, it is necessary to understand grammar and rules of the language used in the software for making the access control file 91c. Otherwise, the access control file 91c that is written incorrectly may cause a wrong access control or may deteriorate the security of the entire WWW server 91.

For this reason, many service providers of the Internet prohibit the access control file 91c from being placed on the directory, or use software that ignores the presence of the access control file 91c.

Therefore, it is difficult to control the access for each information resource by any of the above-mentioned methods.

SUMMARY OF THE INVENTION

An object of the present invention is to provide a network server, a transmission control method and a recording medium for performing an easy and flexible access control to information resources.

A network server according to one aspect of the present invention comprises transmission control means for controlling transmission of a hypertext. The hypertext includes access permission information that is information concerning permission of an access to the hypertext. The transmission control means controls transmission of the hypertext to a client in accordance with the access permission information when the client requests for the access to the hypertext.

Preferably, when transmitting the hypertext, the transmission control means generate a hypertext in which the access permission information is deleted and send the same.

A method for controlling transmission of a hypertext according to another aspect of the present invention is used in a network system including a network server for transmitting the hypertext and a client capable of accessing to the network server. The hypertext includes a description of access permission information that is information concerning permission of an access to the hypertext. The method comprises ~~the steps of~~ deciding whether the hypertext should be transmitted to the client in accordance with the access permission information of the hypertext when the client requests the network server for the access to the hypertext, and transmitting the hypertext when it is decided that the hypertext should be transmitted.

Preferably, when transmitting the hypertext, a hypertext in which the access permission information is deleted is generated to be transmitted.

The recording medium storing the hypertext is a computer-readable recording medium storing a hypertext in which access permission information concerning permission of an access is described.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a diagram explaining the Internet and a WWW system.

Fig. 2 is a diagram showing a screen of a WWW browser.

Fig. 3 is a block diagram showing a functional structure of a WWW server and a terminal device.

Fig. 4 is a diagram showing an example of a description of a hypertext.

Fig. 5 is a diagram showing a dialog box for inputting a user name and a password.

Fig. 6 is a flowchart showing a process of the terminal device.

Fig. 7 is a diagram showing a screen of the WWW browser for displaying a message of denying the access.

Fig. 8 is a flowchart showing a process of the WWW server.

Figs. 9A and 9B are diagrams showing combinations of access control tags.

Figs. 10A and 10B are diagrams showing a conventional WWW system.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Hereinafter, the present invention will be explained more in detail with reference to embodiments and drawings.

Fig. 1 is a diagram explaining the Internet 1 and a WWW system 2. Fig. 2 is a diagram showing a screen HG1 of a WWW browser 22a1. Fig. 3 is a block diagram showing a functional structure of a WWW server 21 and a terminal device 22. Fig. 4 is a diagram showing an example of a description of a hypertext HT. Fig. 5 is a diagram showing a dialog box DAB for inputting a user name and a password.

As shown in Fig. 1, the Internet 1 comprises a communication line 11, a network server 12 that provides various services such as an electronic mail, net news, a file transfer or a WWW, a terminal device 13 that is a client for receiving these services and other various devices or systems.

The communication line 11 comprises a plurality of LANs 11a connected with each other or a public line that connects the terminal device 13 with the LAN 11a. A communication protocol TCP/IP is used for the Internet 1, and a communication protocol HTTP is used in the WWW system 2.

The WWW system 2 is an information providing system using a partial structure of the Internet 1. ~~Especialy, it is realized by~~ According to an aspect of the present invention, the WWW server 21 and the terminal device 22 ~~having the function of as~~ the WWW browser.

The WWW server 21 comprises a server body 21a including a CPU, a RAM, a communication control unit and a magnetic disk drive 21H, a display device 21b and a keyboard 21c. The WWW server 21 is a network server 12 that transmits a hypertext HT responding to an access request from the terminal device 22.

The hypertext HT is a text file described in a language such as HTML or XML for

displaying Web contents on the WWW browser. The information provider describes an information resource to be provided in a language such as the HTML for making a hypertext HT. In this example, the information provider can describe an access control tag TG as shown in Fig. 4 in the hypertext HT, so that the WWW server 21 can perform an access control to the hypertext HT. ~~The detail will be explained later.~~

The magnetic disk drive 21H stores an operating system and application programs necessary for realizing the functions of the WWW server 21 and a document database DBT including a set of the hypertexts HT to be provided for the terminal device 22. These programs or data are loaded in the RAM so that the CPU executes operation.

The terminal device 22 comprises a terminal device body 22a equipped with a CPU, a RAM and a communication device, a display device 22b, a keyboard 22c and a mouse 22d.

The WWW browser 22a1 is installed in the terminal device body 22a.

The WWW browser 22a1 requests the WWW server 21 for an access to the hypertext HT and downloads the hypertext HT. Alternatively, as the screen HG1 shown in Fig. 2, the WWW browser 22a1 displays Web contents for the user visually using characters or images in accordance with the hypertext HT.

In Fig. 2, the user of the terminal device body 22a operates the WWW browser 22a1 for requesting the access to the hypertext HT by inputting a URL of a desired hypertext HT in a text box BX or by clicking a hyperlink HL while viewing the screen HG1 displayed on the display device 22b.

A personal computer or a workstation can be ~~mainly~~ used as the terminal device 22. Other ~~device~~ devices having a WWW browser function such as a cellular phone, a PHS, a game machine or an interactive TV set can ~~be~~ also be used.

Thus, the WWW server 21 and the terminal device 22 have the functions shown in Fig. 3.

As shown in Fig. 3, the WWW server 21 has functions of reception means 211, file searching means 212 and transmission control means 213.

The reception means 211 receives information concerning a request for the access from the terminal device 22 to the hypertext HT. The file searching means 212 searches a hypertext HT corresponding to the request from the document database DBT.

The transmission control means 213 comprises an access permission decision portion 213a, a file generating portion 213b and a file transmission portion 213c. The

transmission control means 213 controls the transmission of the hypertext HT to the terminal device 22.

The access permission decision portion 213a ~~decides~~ determines whether the access to the hypertext HT should be permitted or not in accordance with the access control tag TG included in the hypertext HT. Namely For example, it is ~~decided~~ determined whether the hypertext HT should be transmitted to the terminal device 22 or not. ~~The detail will be explained later.~~

The file generating portion 213b deletes the access control tag TG from the hypertext HT and generates a hypertext HT to be transmitted to the terminal device 22.

The file transmission portion 213c transmits a hypertext HT or a message of refusing the access to the requesting terminal device 22.

The communication control means 221 of the terminal device 22 performs transmission and reception with another device, such as a request for an access to the hypertext HT in accordance with the URL, or reception of the hypertext HT.

Hereinafter, According to an aspect of the present invention, the access permission decision portion 213a, the hypertext HT and the access control tag TG ~~will be~~ are explained in further detail.

In Fig. 4, the hypertext HT is described in the HTML and includes an access control tag TG. The access control tag TG is defined in the HTML beforehand. The access permission decision portion 213a of the WWW server 21 ~~decides~~ determines whether the access to the hypertext HT should be permitted or not in accordance with the argument in the access control tag TG.

The access control tag "<meta access deny [domain 1], ..., [domain k]>" ~~means~~ indicates that an access from a device belonging to the domain designated in the argument [domain k] is denied. Therefore, the access control tag "<meta access deny zzzzz.co.jp>" shown in Fig. 4A ~~means~~ indicates that an access from a domain "zzzz.co.jp" is denied.

The access control tag "<meta access deny [domain 1], ..., [domain k]>" ~~means~~ indicates that an access from a device belonging to the domain designated in the argument [domain k] is permitted.

The access control tag "<meta access passwd [user name 1], [password 1], ..., [user name k], [password k]" ~~means~~ indicates that the access is permitted when the user designated in the argument [user name k] inputs the password designated in [password k].

Therefore, if the user name or the password is not identical, the access is denied.

When the access control tag "<meta access passwd>" is included in the hypertext HT, the access permission decision portion 213a instructs the requesting terminal device 22 to display the dialog box DAB shown in Fig. 5 for the user. The user inputs the user name and the password in the dialog box DAB shown in Fig. 5. Therefore, the access control tag "<meta access passwd John, 7s#Q1" shown in Fig. 4B ~~means~~ indicates the access is denied if the user name "John" and the password "7s#Q1" are not inputted.

Next, an example a process of the access to a hypertext HT will be explained with reference to flowcharts.

Fig. 6 is a flowchart showing a process of the terminal device 22. Fig. 7 is a diagram showing a screen HG2 of the WWW browser 22a1 for displaying a message of denying the access. Fig. 8 is a flowchart showing a process of the WWW server 21.

As shown in Fig. 6, in the terminal device 22, a user designates a URL of a desired hypertext HT by the WWW browser 22a1 (#10). This request and information about the terminal device 22 are transmitted to the WWW server 21 designated in the URL via a DNS server or a relay server in the Internet 1 (#11).

When an input of a user name and a password is requested from the WWW server 21 (Yes in #12), the user inputs the user name and the password in the dialog box DAB to send them to the WWW server 21 (#13).

The hypertext HT or the message of denying the access is received from the WWW server 21 (#14). ~~It depends on the~~ The process performed by the WWW server 21 determines whether that the user receives the hypertext HT or the message which of them.

The received hypertext HT or the message is displayed on the display device 22b (#15). If the desired hypertext HT is obtained, the screen HG1 as shown in Fig. 2 is displayed. When the access is denied, the WWW browser 22a1 displays a message indicating the denial as the screen HG2 shown in Fig. 7 for the user.

In Fig. 8, the WWW server 21 receives the request for accessing to the hypertext HT from the terminal device 22 (#20) and searches the corresponding hypertext HT (#21).

If the hypertext HT is not found (No in #22), an error message is transmitted to the terminal device 22 (#23), and the process is finished.

If the hypertext HT is found (Yes in #22), it is ~~decided~~ determined whether the hypertext HT includes an access control tag TG or not (#24).

If an access control tag TG is not included (No in #24), the hypertext HT is transmitted to the requesting terminal device 22 without delay (#28), and the process is finished. If an access control tag TG is included (Yes in #24), it is ~~decided~~determined whether the access should be permitted ~~or not~~ in accordance with the access control tag TG (#25). For example, in ~~the a~~ case of the hypertext HT shown in Fig. 4A, it is ~~decided~~determined that a request for an access from the terminal device 22 belonging to the domain "zzzzz.co.jp" is denied, and a request for an access from others is permitted. In the case of the hypertext HT shown in Fig. 4B, a user name and a password are ~~demanded of~~requested from the requesting terminal device 22, for ~~deciding~~determining whether the access should be permitted or not.

If the access is permitted (Yes in #26), the access control tag TG is deleted from the hypertext HT (#27), and the hypertext HT having no access control tag TG is transmitted to the terminal device 22 (#28). If the access is not permitted (No in #26), the message of denying the access is transmitted to the terminal device 22 (#29).

According to an example ~~the present~~ embodiment, an access control tag TG ~~concerning~~regarding an access control is directly described in a hypertext HT that is an information resource, thereby the access can be controlled for each hypertext HT easily and flexibly.

In addition, since the hypertext HT in which the access control tag TG is deleted is the hypertext HT that is transmitted to the terminal device 22, unauthorized disclosure regarding information leak about the access control can be prevented.

Moreover, since the access control tag TG is defined by a "meta" tag, the WWW browser 22a1 can display Web contents by skipping the access control tag TG when the hypertext HT is transmitted to the terminal device 22 without deleting the access control tag TG. Therefore, even if the access control tag TG is not deleted, contents of the access control tag TG ~~is not~~are not easily disclosed ~~for by~~ the user.

Furthermore, the domain to which the terminal device 22 belongs can be ~~decided~~determined in accordance with the IP address instead of the domain address. In addition, it is also possible to define the access control tag TG for controlling the access in accordance with the type of the operating system or the WWW browser 22a1 that is used in the terminal device 22.

The access control tag TG can be defined by tags other than the tag "<meta

access>." The access control tag TG can be used in various languages other than the HTML or the XML.

Figs. 9A and 9B are diagrams showing combinations of the access control tags TG.

By combining plural access control tags TG, a developed access control can be performed. For example, in the case of the combination shown in Fig. 9A, an access from the domain "xxxxx.co.jp" is permitted without any condition, while an access from the domain "zzzzz.co.jp" is denied. An access from a domain except the above-mentioned domains is ~~is~~ demanded-requires an input of a user name and a password.

In addition, two or more conditions can be assigned by using an AND operator "&" defined beforehand and by describing as "<meta access condition 1 & & condition k>". For example, in the case of the combination shown in Fig. 9B, an access from the domain "zzzzz.co.jp" is required to input a user name and a password, while an access from the domain "xxxxx.co.jp" is permitted without other conditions.

~~Though-Although~~ the WWW system 2 is provided on the Internet 1 in this example embodiment, it may also, for example, be provided on a local network such as an intranet.

~~Though-Although~~ this embodiment shows an example where the hypertext HT is recorded in the magnetic disk drive 21H, the hypertext HT can be recorded in other media, for example, ~~including~~ a semiconductor memory such as a RAM or a ROM, a portable medium such as a CD-ROM, a floppy disk, a memory card or a magneto-optical disk. If the recording medium is a portable medium, the hypertext HT is read out by the drive corresponding to the type of the portable medium and is stored in a magnetic disk or other media, or is loaded on a main memory for processing.

A structure, process contents and process order in the whole or a part of the WWW system 2, the WWW server 21, or the terminal device 22, or a rule of the access control tag TG can be changed in the scope of the present invention.

~~According to the above-mentioned embodiment~~ aspects of the present invention, an easy and flexible access to information resources can be realized.

While ~~the presently preferred example~~ embodiments of the present invention have been shown and described, it will be understood that the present invention is not limited thereto, and that various changes and modifications may be made by those skilled in the art without departing from the scope of the invention as set forth in the appended claims and their equivalents.